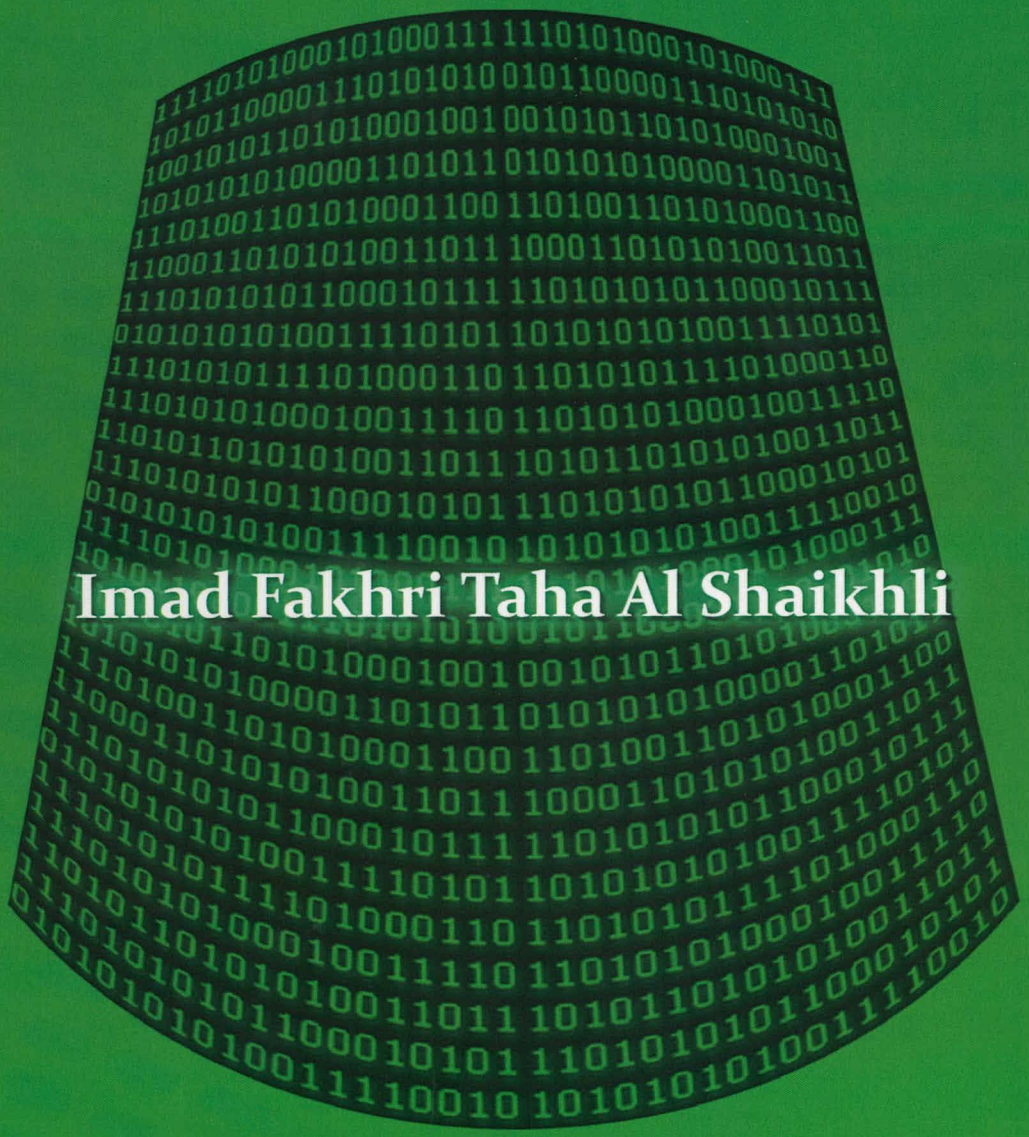
Cryptography

Past, Present and Future

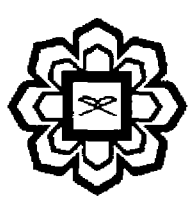


Imad Fakhri Taha Al Shaikhli

IIUM PRESS
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

Cryptography: Past, Present and Future

Imad Fakhri Taha Al Shaikhli



IIUM Press

Published by:

IIUM Press

International Islamic University Malaysia

First Edition, 2011

Perpustakaan Negara Malaysia Cataloguing-in-Publication Data

Imad Fakhri Taha Al-Shaikhli
Cryptography: Past, Present and Future
Imad Fakhri Taha Al-Shaikhli

ISBN: 978-967-418-091-1

Member of Majlis Penerbitan Ilmiah Malaysia – MAPIM
(Malaysian Scholarly Publishing Council)

Printed by :
IIUM PRINTING SDN. BHD.
No. 1, Jalan Industri Batu Caves 1/3
Taman Perindustrian Batu Caves
Batu Caves Centre Point
68100 Batu Caves
Selangor Darul Ehsan

TABLE OF CONTENTS

- Sibomana Hilali Hussein

11. SHA family hash function

- Khanssaa Munthir Abdulmajed
- Sufyan Salim Mahmood Al Dabbagh
- Imad Fakhri Taha Al Shaikhli
- Ahmad Faridi Abdul Matin
- Sibomana Hilali Hussein

ABSTRACT

In this article we will talk about the description of SHA family hash function. Also we will introduce into SHA-0 and its security. Also, we will talk about the SHA-1, SHA-2 and their algorithms. Moreover, we will describe security of the SHA family of hash functions.

DESCRIPTION

SHA-0, SHA-1 and SHA-2 belongs to a family of algorithms designed by the National Security Agency, USA and was published by the US government as a standard (NIST 1994) (Konhiem, 2007). These algorithms were basically inspired by MD4 however several of its blocks are different from that of MD4 (Chabaud & Joux, 1998; Preneel, 2003). The first version was known as SHA-0 (published in 1993) then came the SHA-1(published in 1996) (Turner et al., 2011) and then the SHA2. According to Preneel (2003), the SHA-1 is the most used in today's applications. It is used in Secure Shell (SHH), Secure Socket Layers (SSL) and others. The importance of SHA-1 and SHA-2 has made it necessary to standardize its procedure, hence the SHS (Secure Hash Standard) was published by the National Institute of Standards and Technology (NIST), the latest version is the NIST FIPS 180-3.